UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,805	08/15/2001	Edgardo Gerck	Safevote 1	3666

36743 7590 04/29/2005

MICHAEL HETHERINGTON
P.O. BOX 61047
PALO ALTO, CA 94306

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 04/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/930,805	GERCK, EDGARDO	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-10 are pending.

Specification

1. The abstract of the disclosure is objected to because Page 16, lines 2-3 state that there are less humans living on this planet than 1 billion, when there are approximately 6 billion people living on this planet. Correction is required. See MPEP § 608.01(b).

Claim Objections

2. Claims 1-9 are objected to under 37 CFR 1.75(a) because of the following informalities:

- Claims 1-5 contain different preambles. Select one preamble and use it consistently throughout the dependent claims or simply truncate the preamble to state "a method as in claim 1 further comprising" or the like.
- Claim 1, line 3; claim 6, line 4; and claim 7, line 4 recite the limitation "data base". There is insufficient antecedent basis for this limitation in the claims. For purposes of prior art rejection, "data base" has been construed as "database".
- Claim 7, line 7 recites the limitation "the argument space". There is insufficient antecedent basis for this limitation in the claim. For purposes

of prior art rejection, "the argument space" has been construed as "an argument space".

- Claim 8, line 12 recites the limitation "the registration service". There is insufficient antecedent basis for this limitation in the claim. For purposes of prior art rejection, "the registration service" has been construed as "the registrar service".
- Claim 9, line 4: "reiterate" should be "reiterating".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, and 4-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black (Black, J., "Design for Voting over the Internet: Protocol On Secure Elections", 11/8/1997, pp. 1-5, obtained from http://www.csee.usf.edu/~black/designs/voting.html) in view of Nemes (U.S. Patent 5,287,499).

Regarding Claim 1,

Black discloses a method for generating a unique, one way, compact mnemonic credential for identifying and separately authenticating a voter while maintaining privacy comprising:

Defining a database for identification of voters, wherein the database comprises registration data for each voter (Page 2, Registration, numeral 3);

Defining an authentication record for each voter, assigning a subset from a selected set of characters to each voter in the database (Page 2, Voting Steps, numerals 1-5);

Black does not disclose the use of a collision index for referencing records in the database.

Nemes, however, discloses defining a collision index corresponding to each record in the database, wherein the collision index [pointer] is a number unknown a priori (Column 5, line 63 to Column 6, line 12);

Providing a computer means for calculating the collision index which is used to select a different authentication record, such that each authentication record is unique within a given length (Column 5, line 63 to Column 6, line 12);

Creating thus a one way mapping of a higher dimensional argument space onto a lower dimensional space without collisions such that the mapping cannot be inverted (Column 5, lines 20-25).

It would have been obvious to one of ordinary skill in the art to combine the hashing system of Nemes with the voting system of Black in order to provide a way to store data without collisions that dynamically uses memory (to save the amount of memory used) and that can be searched at fast speeds, even if the table is large (Column 6, lines 13-28).

Regarding Claim 2,

Nemes discloses applying the collision index as part of a hash function used to select a different authentication record, such that each voter authentication record is unique within a given length (Column 5, line 63 to Column 6, line 12); wherein the hash function creates thus a one way mapping of a higher dimensional space onto a lower dimensional space without collisions and so that the hash function cannot be inverted (Column 5, lines 20-25).

Regarding Claim 4,

Black discloses providing a verification key of sufficient length to enable a verifier to authenticate information encoded in the credential while enabling the credential to be made secure against attacks (Page 3, Voting Steps, numerals 11-13).

Regarding Claim 5,

Black discloses providing a local feedback loop, responsive to the collision index for ensuring information encoded in the credential shall be

reliably discovered only by a verifier that has the correct verification key (Page 3, Voting Steps, numerals 11-13).

Regarding Claim 6,

Black discloses a method for generating a unique, one way, compact credential for identifying and separately authenticating a voter over a communication channel while maintaining voter privacy comprising:

Defining a database for identification of voters, wherein the database comprises registration data for each voter (Page 2, Registration, numeral 3);

Defining an authentication record for each voter by assigning a subset from a selected set of characters to each voter in the database (Page 2, Voting Steps, numerals 1-5); and

Translating a credential into a data packet matched to a specific type of communication channel for transporting the credential from a source to a destination along the communication channel (Page 2, Voting Steps, numeral 7).

Black does not disclose the use of a collision index for referencing records in the database.

Nemes, however, discloses defining a collision index corresponding to each record in the database, wherein the collision index is a number unknown a priori (Column 5, line 63 to Column 6, line 12); and calculating a one-way mapping (Column 5, lines 20-25) without collisions from the

collision index such that a different authentication record is selected wherein each authentication record is unique within a given length, and wherein the authentication record provides a credential unique to each voter (Column 5, line 63 to Column 6, line 12). It would have been obvious to one of ordinary skill in the art to combine the hashing system of Nemes with the voting system of Black in order to provide a way to store data without collisions that dynamically uses memory (to save the amount of memory used) and that can be searched at fast speeds, even if the table is large (Column 6, lines 13-28).

Regarding Claim 7,

Black discloses a method for providing a unique, one way voter credential comprising:

Providing a voter database comprising voter registration data for each voter (Page 2, Registration, numeral 3);

Providing a unique voter credential for each voter (Page 2, Voting steps, numerals 1-5);

Providing a voter index corresponding to each voter in the voter database (Page 2, Registration, numeral 3);

Nemes, however, discloses mapping the unique voter credential to the voter index for each voter to create a voter data table (Column 5, lines 10-16); and using a one way function to map without collisions in the result space, each record in the voter data table, to another set of data as a

result space, such that an argument space can have collisions and be larger than the result space and knowledge of the result does not provide knowledge of the voter data (Column 5, line 63 to Column 6, line 12). It would have been obvious to one of ordinary skill in the art to combine the hashing system of Nemes with the voting system of Black in order to provide a way to store data without collisions that dynamically uses memory (to save the amount of memory used) and that can be searched at fast speeds, even if the table is large (Column 6, lines 13-28).

4. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black in view of Nemes, further in view of Kusnick (U.S. Patent 5,892,470).

Black as modified by Nemes does not disclose mnemonic strings.

Kusnick, however, discloses translating the credential into a mnemonic string according to a language rule while preserving credential uniqueness in that language (Column 3, lines 14-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mnemonic encoding system of Kusnick into the voting system of Black as modified by Nemes in order to allow very large numbers to be changed into mnemonic form and be easily remembered by a user (Column 1, line 66 to Column 2, line 4).

5. Claims 8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black in view of Nemes and Kusnick.

Regarding Claim 8,

Black discloses method for automatically generating unique voter credentials at a registrar service that are one-way and short comprising:

Providing a plurality of voter registration files containing private voter data (Page 2, Registration, numeral 3);

Wherein the credential may be used to identify and/or authenticate the voter to a selected third-party and/or to the registrar service without loss of privacy (Page 3, Voting Steps, numerals 8-10).

Black does not disclose the use of a collision index for referencing records in the database or mnemonic strings.

Nemes, however, discloses the following:

Assigning an initial collision index and a header data to each voter file (Column 5, line 63 to Column 6, line 12);

Hashing the voter file with the initial collision index and the header data into a canonical form (Column 5, line 63 to Column 6, line 12);

Folding the canonical form and producing a result with reduced length (Column 5, lines 23-25);

Calculating a modulo division of the result with reduced length (Column 5, lines 23-25);

Ensuring that each credential is unique among all previously calculated credentials (Column 5, lines 20-25). It would have been obvious to one of ordinary skill in the art to combine the hashing system of

Nemes with the voting system of Black in order to provide a way to store data without collisions that dynamically uses memory (to save the amount of memory used) and that can be searched at fast speeds, even if the table is large (Column 6, lines 13-28).

Black as modified by Nemes does not disclose encoding the pre-credential into a desired mnemonic form.

Kusnick, however, discloses encoding the pre-credential into a desired mnemonic form (Column 3, lines 14-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mnemonic encoding system of Kusnick into the voting system of Black as modified by Nemes in order to allow very large numbers to be changed into mnemonic form and be easily remembered by a user (Column 1, line 66 to Column 2, line 4).

Regarding Claim 9,

Nemes discloses verifying whether the encoded credential is unique among all previously calculated credentials for the voter registration files; and if the credential is not unique, assigning a new collision index and reiterating the method by hashing the voter file with the new collision index (Column 7, line 65 to Column 8, line 13).

Regarding Claim 10,

Kusnick discloses translating the credential into a mnemonic string according to a language rule while preserving credential uniqueness (Column 3, lines 14-32).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER